UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/775,537	02/09/2004	Brian Hernacki	SYMAP041	6706

21912 7590 01/18/2008
VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
RYMAN, DANIEL J	

ART UNIT	PAPER NUMBER
2616	

MAIL DATE	DELIVERY MODE
01/18/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/775,537	HERNACKI, BRIAN	
	Examiner	Art Unit	
	Daniel J. Ryman	2616	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 November 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-16 and 18-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-16 and 18-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 February 2004* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Drawings

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: ref. 122 and 124 (see p. 7) and ref. 400 and 412 (see pp. 10-11). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

3. The disclosure is objected to because of the following informalities: on p. 1, ll. 8-9, "transport. Specifically, aspects" should be "transport, specifically, aspects" since the second sentence is a fragment; on p. 3, l. 16 "embodiment; and" should be "embodiment;" and on p. 4, l. 2, "Fig. 6B." should be "Fig. 6B; and" so that the description of Fig. 8 is a clause similar to the

clauses used to describe Figs. 1-7; there is a discrepancy between the subject matter corresponding to ref. 116, where ref. 116 is used to denote a "destination" in p. 6, ll. 6 and 10 and where ref. 116 is used to denote assembled data in p. 6, l. 22 and p. 7, l. 11; on p. 7, l. 9, "NIDS" should be "network intrusion detection system (NIDS)"; on p. 10, l. 4, "offset" should be "offset,"; on p. 11, l. 3, "Figure 5A" should be "Figure 5" since there is no Fig. 5A; on p. 11, ll. 11-12, "occurs, as described below in connection with Figure 5B (510)" should be "occurs (510)" since there is no Fig. 5B; and on p. 12, l. 19, "step 712" should be "step 702".

Appropriate correction is required.

4. The Specification should include a Brief Summary of the Invention. *See* 37 CFR 1.73. *See also* MPEP § 608.01(d). This summary should be separate and distinct from the abstract and should be directed toward the invention rather than the disclosure as a whole. This summary may point out the advantages of the invention or how it solves problems previously existent in the prior art (and preferably indicated in the Background of the Invention). If possible, the nature and gist of the invention or the inventive concept should be set forth. Objects of the invention should be treated briefly and only to the extent that they contribute to an understanding of the invention.

Claim Objections

5. Claim 1 is objected to because of the following informalities: in lines 2-3, "two or more fragments comprising the fragmented network traffic" should be "two or more fragments contained in the fragmented network traffic" because it is assumed that the fragmented network traffic is composed of fragments in addition to the fragments encompassing the anomaly. Appropriate correction is required.

6. Claim 18 is objected to because of the following informalities: in line 3, "two or more fragments comprising the fragmented network traffic" should be "two or more fragments contained in the fragmented network traffic" because it is assumed that the fragmented network traffic is composed of fragments in addition to the fragments encompassing the anomaly. Appropriate correction is required.

7. Claim 19 is objected to because of the following informalities: in line 3, "two or more fragments comprising the fragmented network traffic" should be "two or more fragments contained in the fragmented network traffic" because it is assumed that the fragmented network traffic is composed of fragments in addition to the fragments encompassing the anomaly. Appropriate correction is required.

8. Claim 20 is objected to because of the following informalities: in line 5, "two or more fragments comprising the fragmented network traffic" should be "two or more fragments contained in the fragmented network traffic" because it is assumed that the fragmented network traffic is composed of fragments in addition to the fragments encompassing the anomaly. Appropriate correction is required.

9. Claim 21 is objected to because of the following informalities: in lines 4-5, "two or more fragments comprising the fragmented network traffic" should be "two or more fragments contained in the fragmented network traffic" because it is assumed that the fragmented network traffic is composed of fragments in addition to the fragments encompassing the anomaly. Appropriate correction is required.

Claim Rejections - 35 USC § 112

10. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

11. Claims 18 and 19 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

12. Claim 18 recites: "wherein performing further processing comprises initiating increased buffering of the fragmented network traffic if it is determined that two or more fragments comprises said fragmented network traffic have overlapping portions." Claim 1, which claim 18 depends upon, recites: "initiating in response to detecting said anomaly expanded buffering of said fragmented network traffic; and performing further processing". It is unclear whether the "increased buffering" of claim 18 is synonymous with or distinct from the "expanded buffering" of claim 1. Both claim 1 and claim 18 require the buffering to occur upon a determination of the presence of an anomaly; however, claim 18 clearly requires the buffering as part of the processing step whereas claim 1 clearly requires the buffering to be performed separate from the processing step. For purposes of examination in relation to the prior art, Examiner will interpret claim 18 as "wherein the anomaly occurs when two or more fragments have overlapping portions", where Examiner notes that this interpretation makes claim 18 substantially identical to claim 2.

13. Claim 19 recites: "wherein performing further processing comprises initiating increased buffering of the fragmented network traffic if it is determined that two or more fragments comprises said fragmented network traffic have mismatching overlapping portions." Claim 1, which claim 18 depends upon, recites: "initiating in response to detecting said anomaly expanded buffering of said fragmented network traffic; and performing further processing". It is unclear

whether the "increased buffering" of claim 19 is synonymous with or distinct from the "expanded buffering" of claim 1. Both claim 1 and claim 19 require the buffering to occur upon a determination of the presence of an anomaly; however, claim 19 clearly requires the buffering as part of the processing step whereas claim 1 clearly requires the buffering to be performed separate from the processing step. For purposes of examination in relation to the prior art, Examiner will interpret claim 19 as "wherein the anomaly occurs when two or more fragments have mismatching overlapping portions", where Examiner notes that this interpretation makes claim 19 substantially identical to claim 5.

Claim Rejections - 35 USC § 101

14. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

15. Claim 21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 21 encompasses a signal, per se, because claim 21 requires a "computer program product" where the Specification defines computer program products to include "program instructions . . . sent over optical or electronic communication links," i.e. program instructions sent by signals per se. Specification: p. 5, ll. 4-5. A signal is not a process "because it is not a series of steps." Annex IV of *Interim Guidelines for Examination of Patent Applicaions for Patent Subject Matter Eligibility,* 1300 *Off. Gaz. Pat. Office* 142 (Nov. 22, 2005) (Patent Subject Matter Eligibility Interim Guidelines). A signal is not a machine because it "has no physical structure" and "does not itself perform any useful, concrete and tangible result". *Id.* "A claimed signal is not matter, but a form of energy, and therefore is not a composition of

matter." *Id.* Finally, a signal is not a manufacture because "manufacture" requires some form of matter, which a signal does not have. *Id.* Therefore, a signal, per se, is non-statutory. *See id.* To overcome this rejection, Applicant should delete from the Specification the aforementioned phrase, or Applicant should amend claim 21 in a way that clearly does not permit the program to be embodied on a signal, per se.

Claim Rejections - 35 USC § 103

16. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

17. Claims 1-16 and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pochon et al. (US 2003/0048793), of record, in view of Cantrell et al. (US 2004/0093513).

18. Regarding claims 1, 20, and 21, Pochon discloses a method for assembling fragmented network traffic, comprising: detecting in the fragmented network traffic an anomaly that could result in two or more fragments comprising the fragmented network traffic being reassembled at a monitoring node to obtain a reassembled data flow that is different than a corresponding data as reassembled at a destination node to which the fragmented network traffic is addressed (¶¶ [0089]-[0093], esp. ¶ [0093], where an NIDS checks to determine whether there is a conflict between previously received fragments and a currently received fragment, i.e. check to determine if there is an anomaly, see also ¶¶ [0022]-[0026]); and performing further processing on the fragmented network traffic having the anomaly (¶ [0093], where the fragmented network traffic having the anomaly is discarded).

Pochon does not expressly disclose initiating in response to detecting said anomaly expanded buffering of said fragmented network traffic. Rather, Pochon discloses that in response to detecting an anomaly the fragments are discarded (¶ [0093]). Cantrell teaches, in a system for identifying anomalies in fragmented network traffic (¶ [0026]), that if a "suspicious" packet is identified, i.e. an anomaly is identified, then the packet is set aside for a more careful examination (¶ [0057]), where this permits the system to quickly identify suspicious packets at line rate and then take extra time to detect whether the suspicious packet is benign or malicious to permit the return of benign packets to the transmission line (¶ [0061], see also ¶ [0063]). In addition, Cantrell discloses that the more careful examination includes the use of expanded buffering (¶ [0065], where the more careful examination includes comparing a copy of the suspicious packet to various signatures to determine if the suspicious packet is malicious, see also ¶¶ [0026] and [0062]- [0065], which discloses that the intrusion detection system can consider all options). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to initiate, in response to detecting said anomaly, expanded buffering of the fragmented network traffic to allow a more careful examination of the suspicious packet to determine whether the packet is benign or malicious.

19. Regarding claims 2 and 18, Pochon in view of Cantrell discloses that detecting an anomaly comprises determining that said two or more fragments overlap (Pochon: ¶¶ [0022]-[0026], see also Cantrell: ¶ [0026]).

20. Regarding claim 3, Pochon in view of Cantrell discloses that determining that said two or more fragments overlap comprises reading a header value associated with one of the fragments (Pochon: ¶¶ [0091]-[0092]).

21. Regarding claim 4, Pochon in view of Cantrell discloses that the header value comprises an offset value (Pochon: ¶¶ [0091]-[0092]).

22. Regarding claims 5 and 19, Pochon in view of Cantrell discloses that detecting an anomaly comprises determining that said two or more fragments overlap and that at least two of said fragments comprise different data for an overlapping portion of said fragments (Pochon: ¶¶ [0022]-[0026], see also Cantrell: ¶ [0026]).

23. Regarding claim 6, Pochon in view of Cantrell discloses that performing further processing comprises determining configuration information associated with said destination node (Cantrell: ¶ [0065], where a database of information pertaining to the various machines on the network is located in the intrusion detection system, see also Cantrell: ¶¶ [0026] and [0062]-[0065], where the intrusion detection system determines all options and looks at various protocols when processing the packet).

24. Regarding claim 7, Pochon in view of Cantrell does not expressly disclose that determining configuration information comprises querying the destination node; however, Pochon in view of Cantrell does disclose that determining configuration information comprises gathering such information in any known ways (Cantrell: ¶ [0065]). Examiner takes official notice that querying a node is a known way to gather information on the node. As such, it would have been obvious to one of ordinary skill in the art at the time of the invention to query a destination node since this is a known way to gather information on a node.

25. Regarding claim 8, Pochon in view of Cantrell discloses that determining configuration information comprises querying an information base (Cantrell: ¶ [0065]).

26. Regarding claim 9, Pochon in view of Cantrell discloses that performing further processing comprises reassembling the fragmented network traffic (Pochon: ¶¶ [0039]-[0040]) to generate more than one variant of the reassembled data flow (Cantrell: ¶¶ [0026] and [0062]-[0065]).

27. Regarding claim 10, Pochon in view of Cantrell discloses processing the anomaly to determine whether the fragmented network traffic is associated with a threat (Cantrell: ¶¶ [0065]).

28. Regarding claim 11, Pochon in view of Cantrell discloses performing an action on the fragmented network traffic based on whether the fragmented network traffic is associated with a threat (Cantrell: ¶ [0063]).

29. Regarding claim 12, Pochon in view of Cantrell discloses discarding at least a portion of the fragmented network traffic if the fragmented network traffic is associated with a threat (Cantrell: ¶ [0063]).

30. Regarding claim 13, Pochon in view of Cantrell discloses copying one or more fragments comprising the fragmented network traffic to a buffer (Cantrell: ¶ [0065], where it is implicit that the traffic is copied to a buffer).

31. Regarding claim 14, Pochon in view of Cantrell discloses that performing further processing comprises sending an alert (Cantrell: ¶ [0063]).

32. Regarding claim 15, Pochon in view of Cantrell discloses that performing further processing comprises determining whether the fragmented network traffic should be blocked (Cantrell: ¶ [0063]).

33. Regarding claim 16, Pochon in view of Cantrell discloses that performing further processing comprises determining whether the fragmented network traffic should be forwarded to the destination node (Cantrell: ¶ [0063]).

Conclusion

34. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Daniel J. Ryman whose telephone number is (571)272-3152. The examiner can normally be reached on Mon.-Fri. 8:00am-4:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Huy Vu can be reached on (571)272-3155. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Daniel J. Ryman
Examiner
Art Unit 2616

Daniel Ryman